NOTICE

U.S. Department of Transportation
Federal Aviation Administration

N 8110.94

01/16/01

Cancellation Date: 01/16/02

SUBJ: GUIDELINES FOR THE APPROVAL OF AIRBORNE SYSTEMS AND EQUIPMENT CONTAINING USER-MODIFIABLE SOFTWARE

1. PURPOSE. This notice provides guidelines to Aircraft Certification Office (ACO) engineers and Designated Engineering Representatives (DER) regarding the application of RTCA/ DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," for approval of airborne systems and equipment designed to contain user-modifiable software components. These guidelines are applicable to the approval of airborne systems and equipment and the software aspects of those systems related to type certificates (TC), supplemental type certificates (STC), amended supplemental type certificates (ASTC), amended type certificates (ATC), and Technical Standard Order Authorizations (TSOA). This notice is for guidance purposes only and is supplemental to document DO-178B.

2. DISTRIBUTION. This notice is distributed to the branch level in Washington Headquarters Aircraft Certification Service, section level in all Aircraft Certification Directorates, all National Resource Specialists (NRS), all Aircraft Certification Offices (ACO), all Manufacturing Inspection Offices (MIO), all Manufacturing Inspection District or Satellite Offices (MIDO/MISO), and all Flight Standards District Offices (FSDO). Additional limited distribution should be made to the Air Carrier District Offices, the Aeronautical Quality Assurance Field Offices, and the FAA Academy.

3. RELATED PUBLICATIONS.

a. Advisory Circular 20-115B, "RTCA, Inc. Document RTCA/DO-178B," dated January 11, 1993.

b. RTCA, Incorporated, document RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," dated December 1, 1992.

4. DEFINITIONS.

a. User-modifiable software, as the term is used in DO-178B, is software intended for modification by the aircraft operator without review by the certification authority, the airframe manufacturer, or the equipment vendor, if within the modification constraints established during the original certification project. (Reference DO-178B, paragraph 2.4.)

Distribution: A-W(IR)-3; A-X(CD)-3; A-FAC-0 (ALL), A-FFS-7 (ALL); A-FFS-2,8 (LTD); AMA-220 (25 copies); AFS-600 (3 copies)

Initiated By: AIR-130

NOTE: Modifications by the user to user-modifiable software may include modifications to data, modifications to executable code, or both, if within the modification constraints established during the original certification program.

b. Option-selectable software is software that contains approved and validated components and combinations of components that may be activated by the user, either through selection by the flight crew or activation by ground personnel. (Reference DO-178B, paragraph 2.4.)

c. Field-loadable software is software that can be loaded without removal of the equipment from the installation. Field-loadable software can refer to either executable code or data. (Reference DO-178B, paragraph 2.5.)

5. SCOPE. This notice applies to user-modifiable software only. The guidance provided below does not apply to option-selectable software nor field-loadable software, except where such software is also user-modifiable.

6. THE USE OF EARLIER VERSIONS OF RTCA/DO-178. Versions of DO-178 prior to version B did not provide any guidance regarding user-modifiable software, and should not be used as a means of compliance for user-modifiable software approvals. For software developed to previous guidelines, at least the user-modifiable component, the protective schemes, and any affected aspects of the non-modifiable component should be developed to DO-178B or other acceptable equivalent means as agreed to between the applicant and the ACO. DO-178B guidance for user-modifiable software is contained in Sections 2.4, 5.2.3, 7.2, 11.1, and 11.10 of that document. DO-178B also provides guidance for upgrading software from previous guidance in Section 12.1.4.

7. SAFETY CONSIDERATIONS.

a. User-modifiable software is software within an airborne system approved for user modification. Users (e.g., airlines, operators) may modify user-modifiable software within the specified modification constraints and with approved modification procedures without any further involvement by the certification authority. It is intended that once the system with the user-modifiable software has been certified, the certification authority should require no further visibility, review, or approval of modifications made to that user-modifiable software component. Therefore, modification of the user-modifiable software by the user should have no effect on the aircraft safety margins or operational capabilities, flight crew workload, any non-modifiable software components, or any protection mechanisms of the system.

b. An user-modifiable software component is that part of the software within the airborne system that is designed and intended to be changed by the user. A non-modifiable software component is one that is not designed or intended to be changed by the user. Any change that affects safety margins, operational capabilities, flight crew workload, any non-modifiable software components, protection mechanisms, or software boundaries, or that results in exceeding a pre-approved range of data, parameters, or equipment performance characteristics

warrants rescinding the classification of the software as user-modifiable, and requires design approval under the applicable regulations.

> NOTE: Multiple trim values used as user-modifiable software that may affect safety require special attention. In general, it is not acceptable to simply test the trim value throughout its trim range, because of the uncertainty for acceptability of all the combinations of the trims. In most cases, it is not possible to verify all possible combinations of multiple trims. Therefore, in the case of multiple trims used as user-modifiable software, acceptance of verified sets of trims is generally required.

c. The potential effects of user-modifiable software modification must be determined by the system safety assessment and mitigated by system and software design means, development and verification assurance, approved procedures, and approved tools (if applicable). When evaluating data as part of the DO-178B process, the applicant and the approving FAA office should ensure that the protective mechanisms, verification, and user-modification procedures provide for non-interference of the non-modifiable components and protection integrity. The applicant should obtain the concurrence of the certification office early in the program as to the acceptability of the protective mechanism, protection verification, and modification procedures and tools.

> NOTE: The purpose of the protective mechanism is to ensure that the user-modifiable component does not interfere with the non user-modifiable component. This protective mechanism should be evaluated during the initial approval of the system that contains user-modifiable software. It should be assured that no modification of the software by the user affects the protective mechanism. Section 10 of this notice will further address protection.

8. <u>IDENTIFICATION OF DISPLAYED DATA</u>. Where information is displayed to the flight crew and is derived from user-modifiable software, the information should be identified in such a way to indicate that it has not been approved by the certification authority. In the event that the design or inherent nature of the equipment or user-modifiable component makes the distinction between approved and unapproved information so readily apparent to the flight crew that errors distinguishing the two types of information are reasonably precluded, explicit identification may

not be required. Such identification, where required, should be provided by the non-modifiable component and should allow the flight crew to readily distinguish between information approved by the certification authority and information not approved.

9. MODIFICATION OF AIRCRAFT PERFORMANCE PARAMETERS. An example of modifications that could affect the safety margins, operational capability of the aircraft, or crew workload include modifications of displayed data or other data provided to the flight crew for use in determining aircraft performance parameters. Modification of displayed data or other data provided to the flight crew for use in determining aircraft performance parameters requires certification authority approval. Modification of the user-modifiable component to provide or revise these parameters, regardless of whether they are provided as primary or advisory information, requires certification authority approval. Such a change would warrant rescinding the classification of the software as user-modifiable and would require design approval and part number revision.

10. PROTECTION. Non-modifiable software components of the airborne system should be protected from user-modifiable software components. The system requirements should specify the protection mechanisms which prevent the user modification from affecting system safety, operational capability, or flight crew workload. If the system requirements do not include provision for user modification, the software should not be modified by the user. The protection mechanism should be assigned the assurance level associated with the most severe failure condition of the system as determined by the system safety assessment. If software provides the protection mechanism for user-modifiable software, that software protection should be assigned the highest software level of the system as determined by a system safety assessment. The protection should be such that any modification or failure of the user-modifiable software cannot result in loss of protection. Protection integrity cannot depend on any activities being accomplished by the user. The protection integrity should be such that it can neither be breached accidentally or intentionally. The applicant-provided means of modification of the user-modifiable software should be shown to be the only means by which the modifiable component can be changed.

11. TOOLS USED TO PROTECT NON-MODIFIABLE COMPONENTS.

a. DO-178B, Section 5.2.3, requires that the non-modifiable software components be protected from modifiable components in order to prevent interference with the safe operation of the non-modifiable software components. To enforce this protection, the use of the tools used to make the changes to the modifiable component is allowed. If such tools will be used to enforce this protection, then the following information should be provided to the certification authority for approval:

(1) plans for controlling tool version;

(2) plans for controlling tool usage;

(3) plans for qualifying or verifying the tool; and

(4) procedures for performing modifications to the tool.

b. Software forming a component of the tool and used in the protective function should be developed to the software level associated with the most severe failure condition of the system, as determined by a system safety assessment.

c. Use of software tools for user modifications requires tool qualification and approval of procedures of using and maintaining the tool. Changes to the tool or procedures may require re-qualification of the tool.

12. DATA REQUIREMENTS.

a. The applicant should identify in the Plan for Software Aspects of Certification (PSAC) their intention to develop an airborne system that will contain a user-modifiable software component(s). The PSAC should also describe the means of complying with DO-178B (including the design considerations of DO-178B Section 5.2.3), the protection mechanism, and the means of ensuring the integrity of the protection mechanisms. If software tools will be used for the modification, the PSAC should also identify tool qualification plans or verification procedures to ensure that the tool has modified the user-modifiable software to approved procedures and constraints and has not impacted the non-modifiable software or protection mechanisms.

b. The software design data should specify the design methods and details of implementation for ensuring protection from user modifications.

c. The Software Configuration Index should identify the approved procedures, methods, and tools for making modifications to the user-modifiable software, including tool qualification data, if applicable.

d. The Software Accomplishment Summary should summarize the entire development and verification of the non-modifiable software components, user-modifiable software component(s), protection mechanism, and modification procedures and tools, including tool qualification, if applicable.

13. OTHER CONSIDERATIONS. At the time of the user modification, the user assumes responsibility for all aspects of the user-modifiable software components and tools used for modifying the software, including software configuration management, software quality assurance, and software verification. User modifications should be performed to approved procedures established by the system requirements and software data using approved tools. If the user makes any modification to the non-modifiable software components, the protection mechanisms, the approved procedures, or the approved tools, other than those established by the system requirements and approved procedures; they have violated the type design, and the type certificate of the aircraft may be rescinded.

> NOTE 1: During certification, the ACO should coordinate with that part of the regulatory authorities responsible for approving changes to the aircraft configuration in the field. This helps ensure the practicality and acceptability of the tools and procedures used to control the aircraft configuration.

NOTE 2: A system to track or log software modification that fall under the description in this notice should be considered where appropriate so that both the Certification and Continue Airworthiness aspects of the modifications may be reviewed by the cognizant authorities, as needed.

14. CONCLUSION. The information and procedures described in this notice promote clarification and consistent application the DO-178B guidance on the approval of airborne systems and equipment containing user-modifiable software. This notice does not replace or supersede AC 20-115B or DO-178B.

James C. Jones
Manager, Aircraft Engineering Division
Aircraft Certification Service